2018-06

# Enhancing security behaviour by supporting the user

Furnell, SM



10.1016/j.cose.2018.01.016
Computers and Security
Elsevier

# Enhancing security behaviour by supporting the user

Steven Furnell[1], Warut Khern-am-nuai[2], Rawan Esmael[1], Weining Yang[3], and Ninghui Li[3]

[1] Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, United Kingdom

[2] Desautels Faculty of Management, McGill University, Montreal, Canada

[3] Department of Computer Sciences, Purdue University, West Lafayette, Indiana, United States

## Abstract

Although the role of users in maintaining security is regularly emphasized, this is often not matched by an accompanying level of support. Indeed, users are frequently given insufficient guidance to enable effective security choices and decisions, which can lead to perceived bad behaviour as a consequence. This paper discusses the forms of support that are possible, and seeks to investigate the effect of doing so in practice. Specifically, it presents findings from two experimental studies that investigate how variations in password meter usage and feedback can positively affect the resulting password choices. The first experiment examines the difference between passwords selected by unguided users versus those receiving guidance and alternative forms of feedback (ranging from a traditional password meter through to an emoji-based approach). The findings reveal a 30% drop in weak password choices between unguided and guided usage, with the varying meters then delivering up to 10% further improvement. The second experiment then considers variations in the form of feedback message that users may receive in addition to a meter-based rating. It is shown that by providing richer information (e.g. based upon the time required to crack a password, its relative ranking against other choices, or the probability of it being cracked), users are more motivated towards making strong choices and changing initially weak ones. While the specifics of the experimental findings were focused upon passwords, the discussion also considers the benefits that may be gained by applying the same principles of nudging and guidance to other areas of security in which users are often found to have weak behaviours.

Keyword: passwords, authentication, security nudges, user awareness, human factors

## 1. Introduction

Over the past few years, the importance of information security has become clear for individuals and organizations. Numerous incidents serve as evidence, demonstrating that protecting information assets is no longer an optional duty. However, despite the advance in security technology, the weakest link in the information security realm still lies in end-users (Crossler et al. 2013).

Although several studies have shown that some users may intentionally abuse the information systems (e.g., Siponen and Willison 2009; Willison and Backhouse 2006), ample evidence has suggested that many security incidents occurred out of unintentional mistakes such as

negligence, carelessness, and human errors (Safa and Maple 2016). In addition, from an organisational standpoint, less than a third of companies devote attention towards user education and awareness, which are considered to be crucial baseline elements of cyber security for organisations (Klahr et al. 2017).

One of the reasons that have been commonly cited to explain this behaviour (or the lack thereof) is that users tend to be deliberately lax and unmotivated when it comes to information security issues. At first glance, this claim makes sense as end-users are well-known to have limited knowledge in regards to information security (Adams and Sasse 1999). However, upon closer inspection, there are several issues with our current standard security mechanisms that could play a significant role in this phenomenon. For example, it is widely acknowledged that the password strength meter, which is deployed to help users generate stronger passwords, operates as a black-box and has inconsistent design across multiple websites. As a result, many users are confused about its implications (Carnavalet and Mannan 2015). In addition, users' perception of information security has been shown to mismatch reality (Ur et al. 2016). Therefore, it is plausible that users' lack of knowledge or misperception is only a catalyst that amplifies the symptoms of negative behaviour. Meanwhile, one underlying cause is the poorly designed and implemented security mechanisms. As a consequence, users have not been sufficiently informed and supported to enable them to efficiently engage with the security process.

To address this issue, the literature in computer security has started to examine the behavioural side of the information security problems (e.g., Crossler et al. 2013). Our work extends this approach by proposing that users' security behaviour can be enhanced when the users are properly supported by security mechanisms. Particularly, we survey several techniques in the previous literature that have been shown to assist and improve user behaviour. Following that, we provide evidence from two controlled experiments where users' password generation behaviour is significantly improved when the users are exposed to a carefully crafted support system. The first experiment proposes a password guidance system where several novel forms of feedback are provided to the users, and compares the effect of this to a benchmark scenario in which users are provided no guidance or feedback at all. In the meantime, the second experiment reveals that users not only generate stronger passwords but also are more likely to change their passwords after seeing a warning message from a password strength meter when they understand the context and the meaning of such a message.

## 2. Techniques to Assist and Improve Behaviour

In order to enhance overall system security through the behaviour of end-users, previous literature has proposed several avenues to alleviate underlying issues with user perception. Essentially, there are two primary approaches that can be used to promote secure behaviour, which can be broadly categorised as passive support and active intervention, as below.

### 2.1 Passive Support

The traditional approach to support end-users is to provide passive support such as provisioning of upfront guidance or instruction. The guidance usually serves as a tool to steer the users towards behaviours that are consistent with the security framework or security

policy set by the company (Warkentin and Johnston 2008). Several styles of guidance have been proven to be effective in promoting secure behaviours among end-users. For instance, fear appeals have been shown to impact user intention to comply with recommended computer security actions. However, the impact varies across users due to their perceptions of self-efficacy, response efficacy, threat severity, and social influence (Johnston and Warkentin 2010). In addition, prior works have also argued that users behavior can be improved when they are clear about the scope of the systems and information that are sensitive and rationale behind them (Adams and Sasse 1999). Furthermore, the use of self-assessment checklists that contain extensive questionnaires consisting of control objectives and techniques has also been shown to be effective in providing guidance and improving security behavior (Swanson 2001). Also, serious games that involve cognitive training have been demonstrated to help users create and memorize more secure passwords (Forget et al. 2008). In the meantime, educating end users through training is also recognized as a viable path to supporting them. Interesting examples here include active learning from a capstone course (Conklin 2006), the use of a training program that integrates security awareness training (Charoen et al. 2008), and a creative instructional methods such as the use of simulations (Saunders 2002). However, it is important to note that even though several passive support methods are proven to be significantly effective, one of the issues that still persists, even with the provision of these less traditional approaches, is the lack of attention among end-users. As a result, another approach that has been gaining traction in recent years is to actively interact with end-users to nudge them toward better security behaviours.

### 2.2 Active intervention

Active approaches aim to build upon the foundation provided by passive support, using principles from psychology, human-computer interaction, and behavioural economics to nudge end-users such that their behaviours are in line with the desired ones, or to actively provide them interactive feedback during the course of their action. For instance, a study has shown that soft paternalistic solutions can be employed to counter cognitive biases and enhance privacy-sensitive behaviour in the context of mobile devices usage such as Twitter and location sharing (Balebako et al. 2011). This nudging approach has also been successfully employed in other contexts. For example, a system that aggregates feedback from social groups has been shown to be effective in deterring users from potentially unsafe content (Liu et al. 2014). Furthermore, laboratory findings have demonstrated that nudging has a significant positive impact in prompting users to create better answers to secret questions (Senarath et al. 2016). In the same way, the use of interactive feedback has also been explored as another viable avenue to promote secure behaviour. For example, incorporating fear appeals into a password strength meter has been shown to be effective in pushing users towards creating stronger passwords in a field experiment setting (Vance et al. 2013). Also, interactively highlighting potentially risky domain names has been shown to be effective in preventing users from visiting phishing websites (Xiong et al. 2017). Evidently, this form of assistance is incredibly useful in shaping user behavior and thus has been a focus for both academic researchers and practitioners in the area of information security in recent years.

Among several information security related domains, the field that has received most focus in terms of guidance and nudges is the use of passwords. This is an area in which users have historically been proven to have weak behaviours, thanks to a lack of understanding of the

concept of password ‘strength’, alongside a desire to keep things simple for themselves. This often leads towards the selection of passwords that users consider easy to remember, but which attackers would also find easy to guess. However, while much attention has been given to suggested means for improving matters, relatively few works have attempted to directly quantify the effectiveness of providing different forms of guidance and support.

## 3. Experimental Evidence

This section presents the results of two experimental studies that help to reveal the beneficial effects of providing more effective guidance and feedback. Both are focused around the area of passwords, which significant long-standing experience has clearly shown to be an area in which users do not perform effectively. For example, the classic study from Morris and Thompson (1979) found that, from a sample of almost 3,300 passwords, 86% of them were short and/or single character-type strings**.** More recently, the annual SplashData password survey routinely reveals that users persist in making weak password choices, with ‘123456’ and ‘password’ topping the list in the current version at the time of writing (Slain 2016).

Moreover, prior investigation has revealed the paucity of support that users can receive in practice, with leading websites often failing to provide any guidance to users when selecting their passwords and being extremely variable (and often very limited) in the degree to which good practice is then enforced (Furnell 2014). Even at the time of writing, casual investigation reveals that several such leading sites continue to permit weak practice. For example:

- Facebook accepts the combination of the user’s first name and surname as their password;
- Twitter accepts the string ‘1234567890’;
- Amazon remains content to accept ‘password’ as a valid password choice.

Meanwhile, none of the sites present any upfront guidance to support password selection (although Twitter did at least have a password meter – albeit one that rated the aforementioned choice as acceptable, as illustrated in Figure 1). If this lack of provision is apparent with market-leading sites, it is unlikely that users are being better served in other contexts, and it potentially goes some way to explaining why bad practices persist. As such, it is relevant to consider whether making efforts to change the situation, and improve the level of support, would lead to better password choices as a result.

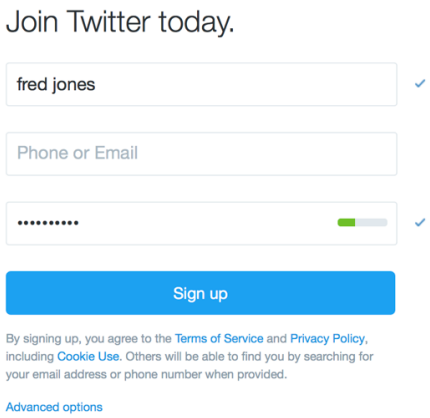



*Figure 1 : Twitter rating 1234567890 as an acceptable password*

Although conducted and analysed independently, the two studies are complementary in terms of their focus and findings. As such, a summary of each approach is presented here, leading to discussion of the key points and the lessons that these studies suggest (not only for passwords, but also for supporting other aspects of end-user security).

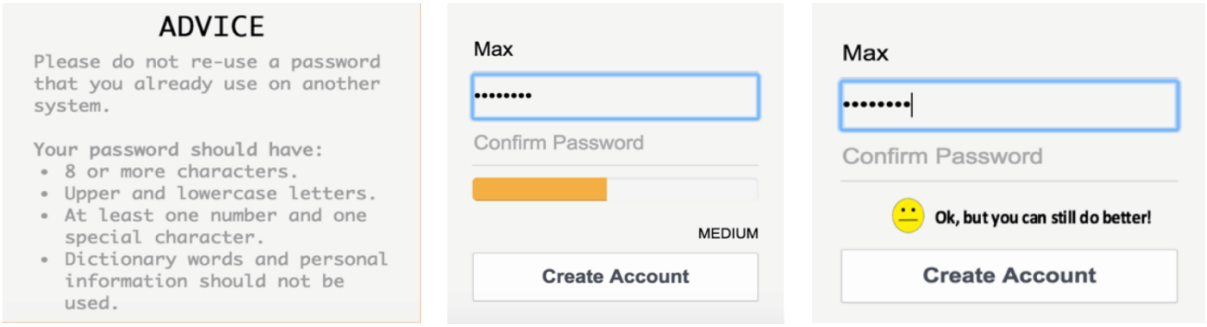
### 3.1 Experiment 1

Based upon positive findings from a small-scale preliminary study (Furnell and Bar 2013), a series of experiments were conducted to determine the extent to which different levels of guidance and feedback would affect end-users' password choices (Furnell and Esmael 2017). A total of 300 participants were involved, and asked to create password-protected accounts in order to register themselves to participate in a survey about social media practices. In this way, the participants were not aware in advance that they were engaging in a study about passwords at all (with the hope that natural behaviour would be observed, as opposed to the sort of artificial good practice that could result from knowing that this was the aspect being measured). This use of mild deception was subject to ethics approval before the experiments commenced. All of the participants were aged 18 or over, and were all general end-users recruited from university, private companies and government organizations (with sampling controls being applied to ensure balance in how they were then assigned within the experiments).

Five alternative scenarios were evaluated (with 60 participants assigned to each one), transitioning from no guidance at all to guidance combined with a novel form of feedback. A key point to note in each case was that there was no enforcement of any password rules; users could choose whatever they liked, and the only difference was the level of guidance and/or feedback provided. The specifics of each scenario were as follows:

1. Passwords were chosen without any guidance or feedback at all, aside from a request not to reuse any existing passwords from other systems (in the hope of enabling genuine password creation behaviour to be observed, albeit with no guarantee that users would heed the request).
2. Four points of basic advice were presented alongside the password selection box (see Figure 1a), reflecting a level of passive support as described in the earlier section.

3. The guidance from scenario 2 was supplemented with a standard password meter under the password entry and confirmation fields, rating password choices as weak, medium or strong (see Figure 1b). This scenario, and those that follow, reflect stepping beyond passive support and into the active intervention category.
4. The meter was replaced with sad, neutral and happy emoji images as an alternative means of rating the suitability of the choices. These were explored to see if users might respond any differently to something more emotional than a password meter (e.g. would they make more effort to try to please the system and get a smiling face?).
5. The emojis accompanied with an emotive feedback message (e.g. "This is not good enough!" for weak password choices), again differentiating the style of feedback from the standard weak-medium-strong approach to ratings (see Figure 1c).




(a) (b) (c)

*Figure 2 : Interface examples from password guidance and feedback study*

The resulting password choices were scored via a utility obtained from GitHub (Mohamed 2014), using the rules shown in Table 1 (noting that if passwords scored over 100, the value was then capped). Three scoring ranges were then used to denote weak, medium and strong choices, thereby enabling a broad comparison between the effectiveness of the different guidance/feedback scenarios. It should be noted that, for the purposes of this study, the underlying specifics of the scoring did not matter too greatly (and so there was no driver to ensure that the rating utility was complying with rules from other methods used elsewhere). The main requirement was for its output to be suitable to then define three meaningful rating categories, as it was these that would drive the assessment of password choices and the ratings presented to users in scenarios 3-5. As the table shows, the scoring process still applies a series of reasonable rules, serving to take account of both length and character composition in the process

| Rules | Rating | Examples | |
|---|---|---|---|
| | | Password | Score |
| • **5 pts** - unique character<br>• **2 pts** – repeated character (one already used anywhere else in the password)<br>• **15 pts** – each time a new character type is included (uppercase letter, lowercase | 0 - 40<br>Weak | 1234567<br>iloveyou<br>luke33 | 35pts<br>37pts<br>37pts |
| | 41 - 70<br>Medium | Luke23<br>BROK3R-foL34p! | 50pts<br>52pts<br>65pts |

| | | | |
|---|---|---|---|
| letter, number or symbol) after the first type used in the password | 71 - 100 Strong | maggie9876543<br>neBemvor1893<br>Lafe@9856!e | 72pts<br>77pts<br>82pts |

*Table 1 : Password scoring rules, rating ranges and examples*

Figure 3 illustrates the breakdown of ratings across the five scenarios, and the results clearly show a dramatic difference between the unguided and guided scenarios. Most notable is the decline in weak choices, falling from 75% in the first scenario down to around a third in the final one (in parallel, passwords rated as strong increased from none in the first instance up to 12% as a result of guidance and feedback). In terms of the chosen passwords themselves, the average length increased from 6.7 characters in the unguided scenario up to 8.8 in the scenario with guidance and emoji-based feedback, with the character diversity also having increased).

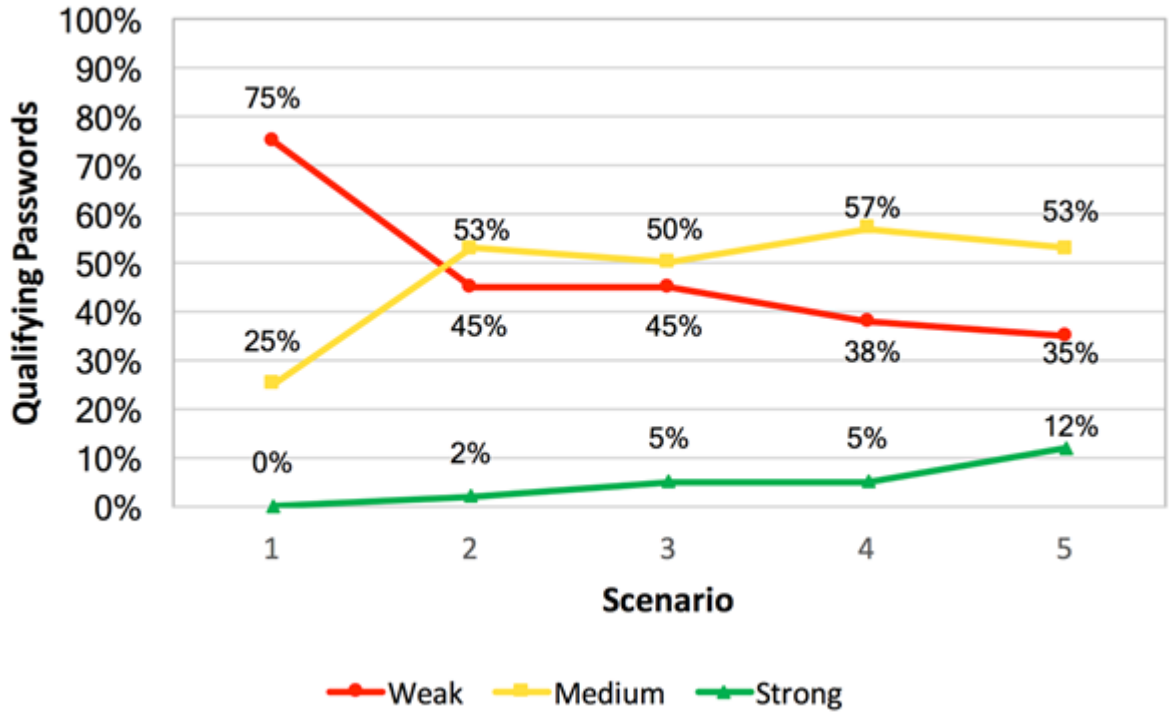



*Figure 3 : Comparing the strength of password choices achieved using different levels of guidance and feedback*

### 3.2 Experiment 2

While the focus of Experiment 1 was whether guidance and feedback had an effect, the basis of Experiment 2 was more specifically geared towards assessing whether password-generating behaviour could be enhanced by giving users more insights into *why* their choices would have an effect upon the resulting security. As such, rather than just providing ratings to denote the strength or sufficiency of the proposed choice, the users were provided with more explanatory detail about how well the resulting password would serve them. Conceptually, this is nothing new, and indeed almost three decades ago Klein proposed the idea of a proactive password checker that "would also have to tell the user *why* a particular

password was unacceptable, and give the user suggestions as to what an acceptable password looks like" (Klein 1990). In practice, however, such explanation is still not routinely provided, and it is relevant to understand whether it would make a difference to users.

A controlled laboratory experiment was conducted to examine how contextual information aids users in improving their password generation behaviour (Khern-am-nuai et al. 2017). The experiment involved 500 US-based participants on Amazon Mechanical Turk that are 18 years old or above. They were asked to create a password to protect their hypothetical account. The only requirement of the password was that it had to have at least 6 characters. At the password generation page, there was a password strength meter that calculated and showed the strength of the password, which was calculated using the Backoff Markov model (Ma et al. 2014). Each user was randomly assigned to one of the four types of the password strength meter, which were chosen based on theoretical supports from the literature and the practicality of real-world implementation. The details of each type are as follows:

1. **Control:** the password strength meter calculates the strength of the password and displays the label of the strength as either "Weak", "Medium", or "Strong".
2. **Time:** the password strength meter calculates the strength of the password and display the label of the strength along with the estimated time to use the brute-force approach to crack that password. An example of the message for this treatment is "Weak. We estimate that it takes 10 seconds to crack your password, assuming that the attacker can try 100 passwords every second".
3. **Rank:** the password strength meter calculates the strength of the password and displays the label of the strength along with the rank of that password compared with their peers. An example of the message for this treatment is "Weak. We estimate that the password you chose is among the 400 weakest passwords".
4. **Probability:** the password strength meter calculates the strength of the password and displays the label of the strength along with the estimated number of accounts that share the same password with the one entered. An example of the message for this treatment is "Weak. We estimate that about 10,000,000 other accounts will have the same password as you within 10 billion accounts".

There were 116 participants assigned to the Control treatment, 133 to the Time treatment, 131 to the Rank treatment, and 120 to the Probability treatment. The interface of the password generation page is shown in Figure 3, illustrating the presentation of the basic rating from the Control version of the experiment. Apart from the specifics of the warning message, the other variants of the meters had the same interface. For example, instead of simply seeing "Weak", users in the Time version would see a more descriptive message as described above. As such, any differences in the results observed would be assumed to be linked only to the nature and level of feedback that the users received.

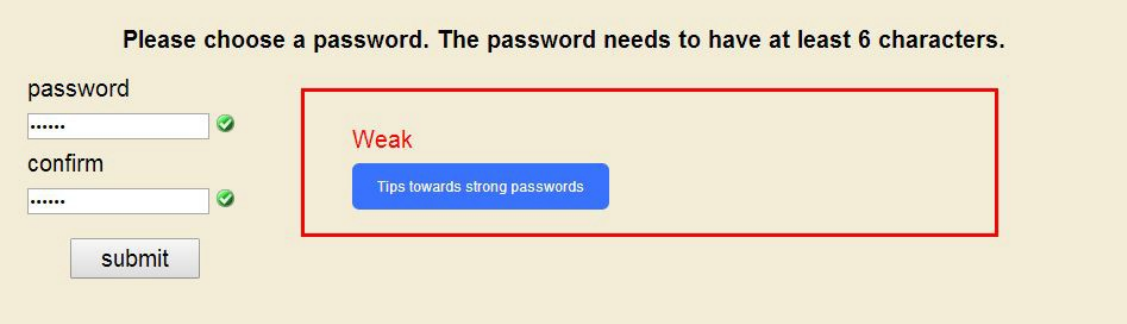



*Figure 3: The interface of the Password Generation page and the Control version of the meter*

All the password-generating activities (e.g., the original password, the revised password, number of occasions the users change their password, number of occasions the users click the "Tips towards strong passwords" button) were recorded. In addition, after submitting the final password of their choices, the users were asked to participate in a non-trivial survey regarding their password generation strategy. After the survey (which takes 30-60 minutes), the users were asked to verify the password they submitted, with the intention that any users who failed this post-test survey would be removed from the dataset. However, none of the users failed the test, enabling all data to be retained. Then, the effectiveness of the context-based password strength meter was tested by comparing with that of the traditional password strength meter (i.e., the control group). The ANOVA test and the post-hoc Tukey HSD Test were utilized for this purpose.

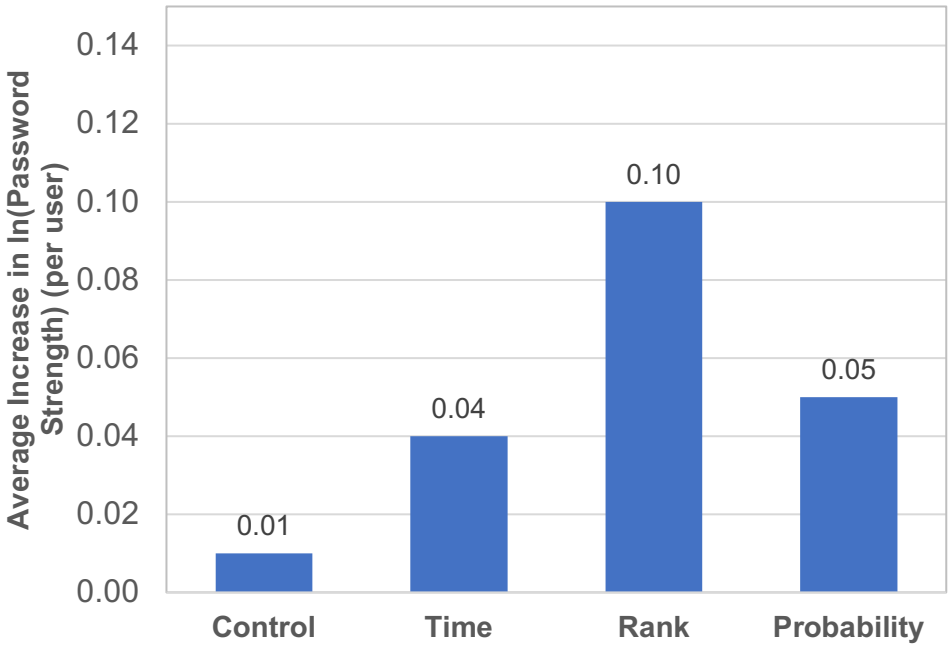



*Figure 4: Average increase in Password Strength for alternative meters*

Figure 4 demonstrates the average increase in password strength based on different types of password strength meters. The natural logarithm was applied to this variable as it is highly skewed by nature. The results show that users who are exposed to contextual information have better understanding of the warning message generated by password strength meters. As a result, users under all context-based password strength meter treatments generally create

stronger passwords compared to those under the traditional meter (i.e. where only the basic strength rating is displayed). However, only the difference of Rank treatment is statistically significant at p-value < 0.01.

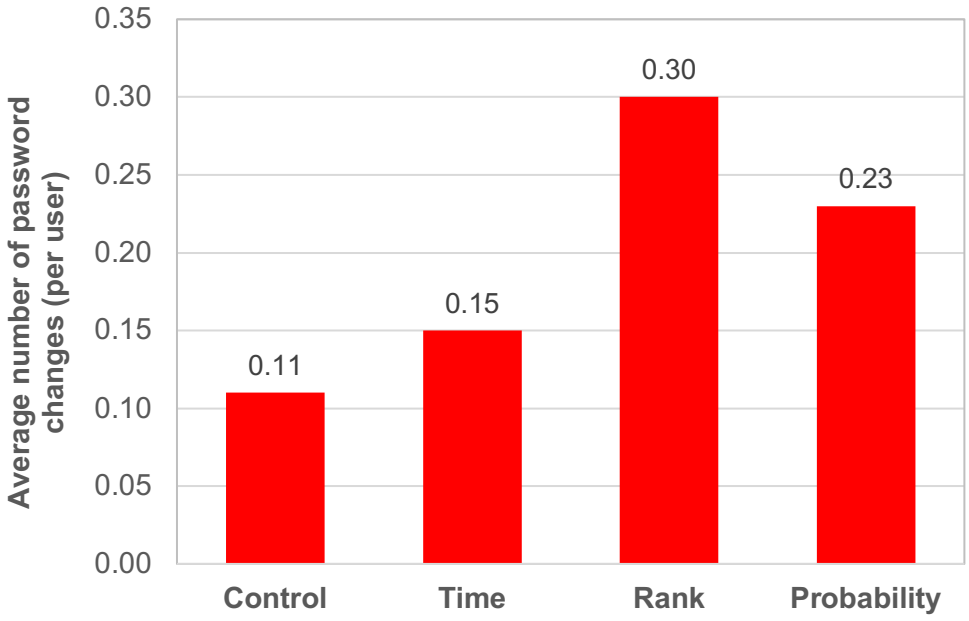



*Figure 5: Average number of password changes for alternative meters*

Similarly, Figure 5 shows the average number of occasions where participants change their passwords immediately after observing the warning generated by password strength meters. Evidently, users under all context-based meter treatments are generally more likely to change their password immediately after observing the warning message compared with those under the traditional password meter. Nevertheless, the difference between the Rank treatment and the control is the only one that is statistically significant at p-value < 0.05.

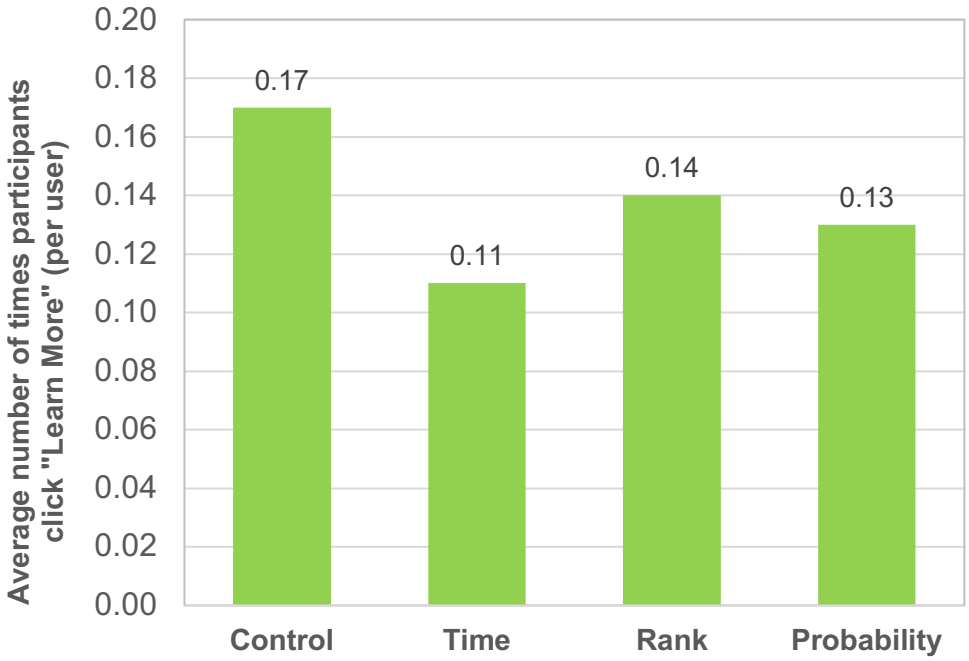



*Figure 6: Average usage of the password tips link across alternative meters*

Figure 6 shows the average number of occasions where users click the "Tips towards strong passwords" button. Interestingly, there is no significant difference here. In fact, users under the traditional password meter are slightly more likely to click the link (potentially indicating that those users experiencing the more explanatory feedback messages already considered themselves to be better informed than those only receiving basic ratings). This finding demonstrates that the password strength meter can be used as a tool to facilitate user education regarding password generating practice. Evidently, including the link that allows users to learn more about how to create stronger passwords is found to be potentially beneficial across all variants of the meter, and again illustrates that if additional provision is made to support the user, then a tangible proportion of them are likely to take advantage of it.

## 4. Findings and implications

Enhancing user security behaviour, including password-generating behaviour, is one of the most important areas in information security research. Many studies have shown that users tend to ignore security guidelines, resulting in elevated risk profiles. Herley (2009) explains such a phenomenon from economic perspectives that users may be resistant to security advices because the cost of following the advice is higher than the benefits. The combined results from the studies show that users actually respond to the "nudges" (i.e., indirect advice) as their behaviour is significantly improved once the nudges are provisioned.

Although it may be argued that no amount of help is likely to change matters for some users, prior research has clearly indicated that there is a tangible proportion of users for whom additional support and guidance could be the key that unlocks compliant behaviour. For example, a survey of over 400 end-users by Furnell et al. (2007) revealed that only four out of ten of them considered that they were in the position of understanding and devoting appropriate time to security. Amongst the rest, a variety of barriers were cited, and key points were lack of understanding of *why* it was necessary or *how* to do it. By contrast very few respondents dismissed the importance of security or indicated that they did not see a need for the controls. Similarly, Furnell et al. (2008) explored this further via a series of interviews with self-categorised novice users, and many considered their own lack of knowledge – rather than a resistance to security – as being a key factor in limiting their protection. Such findings provide justification for the work reported here, as well as various wider efforts to improve the usability and the user experience in relation to security (Wash and Zurko 2017).

While the results from Experiment 1 are still far from perfect, they provide a clear illustration of a positive effect upon user behaviour. Moreover, it can be noted that the guidance was still only telling users *what* to do; if it was further supplemented by giving them an explanation of *why* the guidance was relevant (e.g. briefly describing the difference it makes to password strength) then even more users may have been convinced to comply. This indeed is borne out by some of the findings from Experiment 2, where more descriptive feedback about the quality of the password, its likely resilience to attack, and how it compares to others, are all shown to motivate better selections as a result.

At the same time, the findings do *not* provide definitive evidence that the observed improvements in user behaviour were necessarily caused by them becoming more security

conscious. Indeed, they may have been motivated by the encouragement from the meter, the amusement value of the emoji images, or by the information they received – none of which means they would necessarily have come away more motivated by security itself (or indeed being more security aware). Nonetheless, whatever the motivation, they key point is that it served to change their behaviour in a way that had a positive effect upon security as a result.

In practice, of course, the guidance would not be used in isolation, and would be accompanied by some enforcement of password rules. It can of course be argued that the highest level of compliance could be achieved irrespective of guidance and feedback, by simply enforcing such rules, and preventing weak choices from being accepted. This is indeed the situation faced on many websites, where guidance is often entirely lacking. However, this essentially risks leaving the user feeling like an uninformed victim, forced to follow a process that they do not fully appreciate or understand, and could lead to unintended consequences (Burr et al. 2011). Combining effective guidance and feedback with suitable enforcement is clearly the better solution, and it would seem obvious to say this were it not for the fact that it plainly has not been the norm in so many cases.

The findings align with other recent work in the domain, most notably a study from Segreti et al. (2017) that present adaptive password creation policies that can dynamically change the requirements over time and a study from Ur et al. (2017), with a password meter offering real-time feedback and advice to help users refine their password choices. As with Experiment 2, the principle here is not to just indicate that a password is weak, but to explain why and (importantly) what to do in order to improve it. The findings confirmed a positive effect upon user performance compared, with the data-driven feedback leading to stronger password choices as a result.

Looking beyond passwords, it is also possible to note the effectiveness of providing guidance, nudges and feedback in other contexts. As an example, another recent study from amongst the authors looked at the effect of enhancing the information available to users when selecting and connecting to Wi-Fi networks (Mahmoud et al. 2017). Four alternative interfaces were tested, ranging from a version that mimicked the standard Windows Wi-Fi network selection interface, through to versions with security ratings and additional guidance. The aim was to determine the extent to which the additional information affected user decisions when presented with a range of available networks to connect to. The findings revealed a tangible improvement amongst the users that were exposed to the interfaces offering and promoting more security-related information, again revealing that the presence of such information can have a beneficial approach for security-related decisions.

This, in turn, highlights the desirability of applying the same principles to other areas of security in which awareness-raising support would be useful (i.e. in terms of other areas for which we can show evidence that users do not do well). For example:

- **Software updating**: Rather than simply indicate that package XYZ needs updating, show the user a measure of how out of date their system is (what proportion is out of date, and how out of date it is), and – if appropriate - an indication of how many times the decision to update has been deferred. The latter in particular is something that may be effective in ‘guilting’ users into accepting that they have already postponed the action on previous occasions (for which they may have lost track of the degree to which they had done so). It is also feasible to imagine a situation in which the user is

also provided with an indication of the extent to which unpatched systems have been rendered vulnerable to attacks as a result (e.g. indicating the number of known malware strains that are now exploiting the vulnerability that a given patch seeks to rectify). A similar approach could also be applied with backup; giving the user a metric for how many or what proportion of their files have not been safeguarded (particularly relevant if the system has not been configured to perform backup automatically and relies upon any manual decision from the user). This will give users a more specific feel about the vulnerability of their assets, with the aim of using their own increased awareness as a means of encouraging action.

- **Malware protection**: Rather than just notifying the user that signatures need updating, it would be possible to provide them with additional indicators that would motivate their interest to do so. For example, they could be given a measure of how many known strains of malware their system has protected them against, and an indication of how many new (and thus unknown to their system) strains have been released since their last update. Such insights would provide a more tangible measure than simply giving a generic warning that their protection is 'out of date', while at the same time helping to foster a greater understanding of the problem that they are seeking to address (in the same way that giving password feedback around the rank or time to crack it, as in Experiment 2, is more informative than simply saying that the chosen string is 'weak').

The aim in both cases would be to instil a more tangible sense of mounting vulnerability and risk, which, in turn, would hopefully motivate users to better understand the situation and to take the desired actions in response. Of course, it could be argued that, rather than trying to persuade the user to act, these decisions ought to be taken out of their hands altogether and systems to update without requiring their permission or intervention. This is the route adopted in Windows 10, where the user is basically told that updates will be downloaded and installed automatically (with the only real user-facing option being the ability to specify their 'active hours', so that the system does not attempt to interrupt them with restarts while they are working). This is in notable contrast to the approach in earlier versions of the OS, where the user had ample opportunity to configure their system in a way that could defer updates for a long time. The resulting automation certainly helps to ensure that systems are updated and patched in a timely manner, but the move was not uniformly well-received by the user community, with some users complaining that updates applied without their explicit consent had served to introduce incompatibilities and led to loss of data (Claburn 2017). This serves to illustrate that, as with many aspects of security, there is no panacea for all scenarios, and if automation cannot be relied upon to take decisions out of the hands of users, then it remains relevant to find ways to motivate them to take action themselves.

Lastly, it is also important to note that even after the support is provided, some users may remain guidance-resistant, and will indeed still choose a course of action that works against security. Motivating factors here may include laxity, disobedience, or simply a belief that their personal contribution towards security will make little difference. In addition, the nudge and guidance are provided in the manner in which the presentation and/or implementation make it undesirable to use (Schneier 2013). In that regard, it is also as important to get the usability and design of the security system right in the first place, so that guidance and nudges can serve their own purposes to the fullest extent.

## 5. Conclusions

A common weakness in the provision of security is that while relevant features are present and available to be employed, users are often expected to use them with little upfront guidance, or ongoing support or encouragement. It is therefore hardly surprising to find that users' resulting behaviours are sub-optimal, and often explicitly insecure, if they have been largely left to fend for themselves. The main tenet of this paper is that the situation can be improved by providing users with guidance, feedback, and explanation for their security options and decisions. Such provision can be broadly equated to supporting the learning continuum of awareness, training and education; each provides a step up in terms of users' likely acceptance and resultant compliance, along with the opportunity to positively affect their longer-term security behaviours.

As the specific technology selected for the main focus of this discussion, passwords are widely criticised and frequently dismissed as ineffective security. However, the findings have collectively shown that efforts towards improving user awareness and understanding are then rewarded by better usage. Indeed, it is evident from the two experimental studies that users who are guided by such approaches tend to create stronger passwords compared to those who are unguided. This in turn suggests that users may not ignore the information security issue completely as per conventional wisdom. On the other hand, when security mechanisms they use have properly designed user support, their behaviour can be significantly improved, thus enhancing the overall security of the information system.

It should be reiterated this does not necessarily mean that users have become more aware or accepting of security (although, of course, the efforts to raise their awareness *may* have helped them to do so). What is seen is an improvement in their security-related *behaviours* as a result of awareness-raising efforts. So, regardless of *why* it has motivated them, the use of such interventions and nudges *is* having the desired effect in terms or moving their behaviours in the right direction. Taking it to the extreme, one could argue that organisations do not need to care whether their staff properly understand security, as long as they do the right things. While the authors would not rule out the potential for the interventions to also have a more lasting effect upon users' understanding, the current studies cannot prove this is the case. As such, it is just their direct behavioural response that is in focus.

What can also be said is that the findings provide a lesson not only for passwords, but for end-user security in general. The combination of effective guidance *and* enforcement gives users the chance to understand and buy-into security, but still ensures a safety net for handling those that seek to resist or remain oblivious.

## References


Adams, A., and Sasse, M. A. 1999. "Users Are Not the Enemy," *Communications of the ACM* (42:12), pp. 40--46.

Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L. F., and Sadeh, N. 2011. "Nudging Users Towards Privacy on Mobile Devices," *Proceedings of the CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*.

Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S., and Nabbus, E. A. 2011. "Sp 800-63-1. Electronic Authentication Guideline."

Carnavalet, X. D. C. D., and Mannan, M. 2015. "A Large-Scale Evaluation of High-Impact Password Strength Meters," *ACM Transactions on Information and System Security* (18:1), pp. 1--32.

Charoen, D., Raman, M., and Olfman, L. 2008. "Improving End User Behaviour in Password Utilization: An Action Research Initiative," *Systemic Practice and Action Research* (21:1), pp. 55--72.

Claburn, T. 2017. "'Windows 10 Destroyed Our Data!' Microsoft Hauled into Us Court." Retrieved 22 August, 2017, from https://www.theregister.co.uk/2017/03/24/microsoft_windows_10_update/

Conklin, A. 2006. "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course," *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, pp. 220b--220b.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90--101.

Forget, A., Chiasson, S., and Biddle, R. 2008. "Lessons from Brain Age on Password Memorability," *Proceedings of the 2008 Conference on Future Play: Research, Play, Share*: ACM, pp. 262-263.

Furnell, S. 2014. "Password Practices on Leading Websites–Revisited," *Computer Fraud & Security* (2014:12), pp. 5-11.

Furnell, S., and Bar, N. 2013. "Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers," *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 217--225.

Furnell, S., Bryant, P., and Phippen, A. D. 2007. "Assessing the Security Perceptions of Personal Internet Users," *Computers & Security* (26:5), pp. 410-417.

Furnell, S., and Esmael, R. 2017. "Evaluating the Effect of Guidance and Feedback Upon Password Compliance," *Computer Fraud & Security* (2017:1), pp. 5--10.

Furnell, S., Tsaganidi, V., and Phippen, A. 2008. "Security Beliefs and Barriers for Novice Internet Users," *Computers & Security* (27:7), pp. 235-240.

Herley, C. 2009. "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proceedings of the 2009 workshop on New security paradigms workshop*: ACM, pp. 133-144.

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549--566.

Khern-am-nuai, W., Yang, W., and Li, N. 2017. "Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment," in: *50th Hawaii International Conference on System Sciences*.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., and Wang, D. V. 2017. "Cyber Security Breaches Survey 2017 Main Report."

Klein, D. V. 1990. "Foiling the Cracker: A Survey of, and Improvements to, Password Security," *Proceedings of the 2nd USENIX Security Workshop*, pp. 5-14.

Liu, J., Ruohomaa, S., Athukorala, K., Jacucci, G., Asokan, N., and Lindqvist, J. 2014. "Groupsourcing: Nudging Users Away from Unsafe Content," *Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational*, pp. 883--886.

Ma, J., Yang, W., Luo, M., and Li, N. 2014. "A Study of Probabilistic Password Models," in: *Security and Privacy (SP), 2014 IEEE Symposium on*. pp. 689--704.

Mahmoud, N., Furnell, S., and Haskell-Dowland, P. 2017. "Towards Targeted Security Awareness Raising," *Proceedings of the 16th Annual Security Conference*, Las Vegas, NV.

Mohamed, K. 2014. "Password-Meter-Tutorial." from https://github.com/lifeentity/password-meter-tutorial

Morris, R., and Thompson, K. 1979. "Password Security: A Case History," *Communications of the ACM* (22:11), pp. 594-597.

Safa, N. S., and Maple, C. 2016. "Human Errors in the Information Security Realm--and How to Fix Them," *Computer Fraud & Security* (2016:9), pp. 17--20.

Saunders, J. H. 2002. "Simulation Approaches in Information Security Education."

Schneier, B. 2013. "On Security Awareness Training." Retrieved 2017-11-08, from https://www.darkreading.com/risk/on-security-awareness-training/d/d-id/1139381

Segreti, S. M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L. F., and Mazurek, M. L. 2017. "Diversify to Survive: Making Passwords Stronger with Adaptive Policies," *Symposium on Usable Privacy and Security (SOUPS)*.

Senarath, A., Arachchilage, N. A., and Gupta, B. 2016. "Security Strength Indicator in Fallback Authentication: Nudging Users for Better Answers in Secret Questions," *International Journal for Infonomics* (9:4), pp. 1228--1232.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp. 267--270.

Slain, M. 2016. "Announcing Our Worst Passwords of 2016." from https://www.teamsid.com/worst-passwords-2016/

Swanson, M. 2001. "Security Self-Assessment Guide for Information Technology Systems," Defense Technical Information Center.

Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L. F., Dixon, H., Emami Naeini, P., and Habib, H. 2017. "Design and Evaluation of a Data-Driven Password Meter," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*: ACM, pp. 3775-3786.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., and Cranor, L. F. 2016. "Do Users' Perceptions of Password Security Match Reality?," *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*: ACM, pp. 3748-3760.

Vance, A., Eargle, D., Ouimet, K., and Straub, D. 2013. "Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment," *Proceedings of the 46th Hawaii International Conference on System Sciences*, pp. 2988--2997.

Warkentin, M., and Johnston, A. C. 2008. "It Governance and Organizational Design for Security Management," *Information security: Policies, processes, and practices*), pp. 46--68.

Wash, R., and Zurko, M. E. 2017. "Usable Security," *IEEE Internet Computing* (21:3), pp. 19-21.

Willison, R., and Backhouse, J. 2006. "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective," *European Journal of Information Systems* (15:4), pp. 403--414.

Xiong, A., Proctor, R. W., Yang, W., and Li, N. 2017. "Is Domain Highlighting Actually Helpful in Identifying Phishing Web Pages?," *Human factors* (59:4), pp. 640--660.